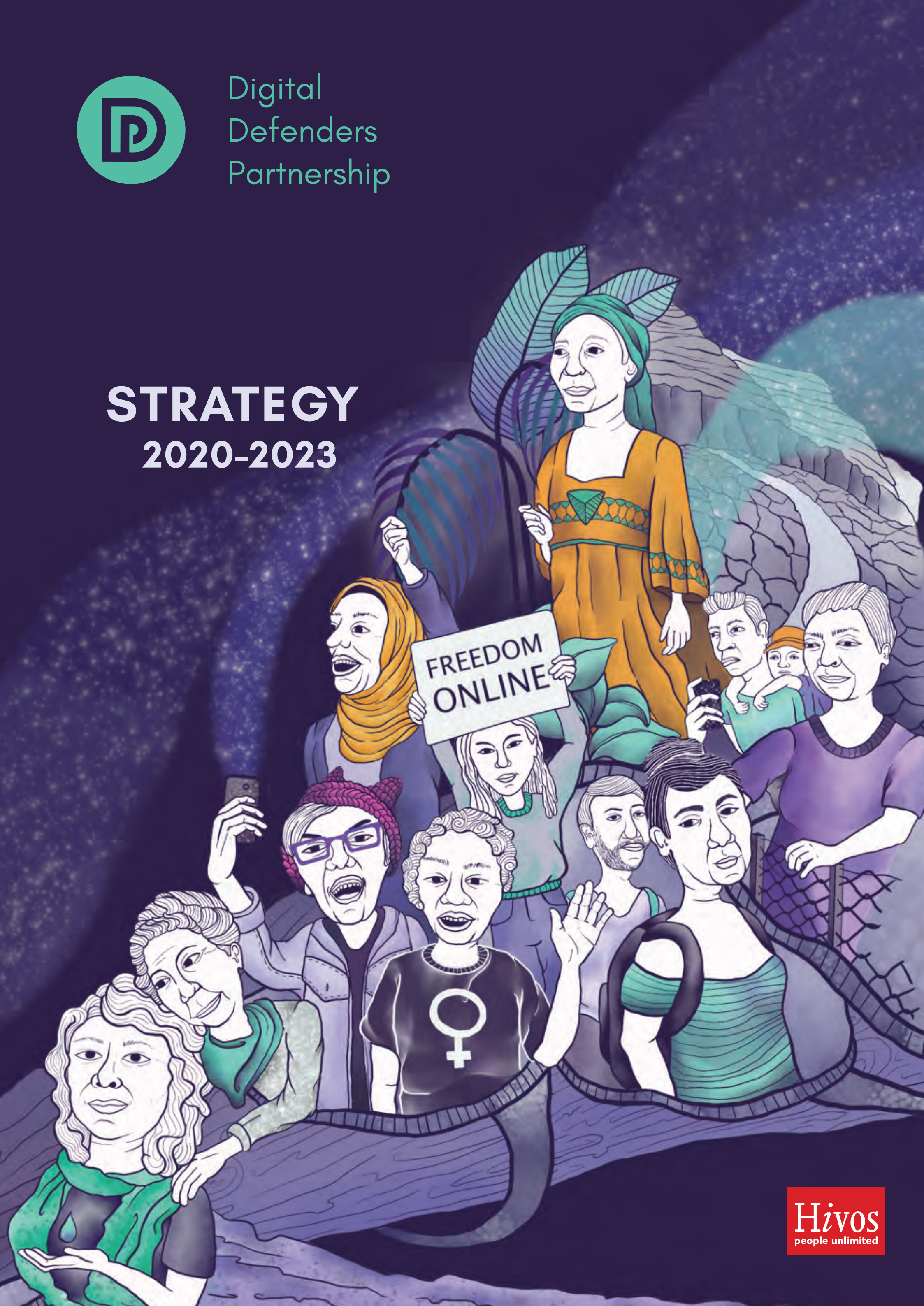
Digital
Defenders
Partnership

STRATEGY
2020–2023



Hivos
people unlimited

Table of Contents

Digital Defenders Partnership

team@digitaldefenders.org

www.digitaldefenders.org

@DigiDefenders

hosted by HIVOS - www.hivos.org

+31 (0)70 376 55 00

Designer: Diana Moreno

https://www.behance.net/dianamoreno

Executive Summary

Seven years since the establishment of the Digital Defenders Partnership by the Freedom Online Coalition, the challenges to Human Rights and Internet Freedom globally have mounted, while the movements in their defence remain diverse, creative, and resilient. In this context, DDP has evolved to become a flexible and effective ally in the ecosystem of support to these movements, expanding our programme of support from emergency funding to include creative and innovative projects aimed at supporting and respecting this diversity, creativity, and resilience.

In the coming strategic period, DDP will focus on the consolidation and expansion of the aspects of our work considered to be of most value by our allies and beneficiaries:

- *Incident Emergency Response*
- *Sustainable Protection Support*
- *Facilitation and Community Building.*

We will do this by increasing clarity and transparency in how we work; facilitating and actively promoting collaboration within the ecosystem; further deepening our support for local and regional capacities; and establishing mechanisms for learning and sharing best practices. All of this with the aim of ensuring that the Internet and digital technologies remain a fundamental force for positive change – free, open and accessible to those on the front lines of that change.

I. DDP: Who we are

History

The Digital Defenders Partnership (DDP) was initiated in late 2012 by the Freedom Online Coalition (FOC) to protect critical Internet users – human rights defenders (HRDs), including activists, bloggers, civil society organisations, journalists, and other users of Information and Communication Technologies (ICT) to defend human rights, and keep the Internet free and open.

From 2012 to 2019, DDP received its funding from the Ministries of Foreign Affairs of Australia, Canada, Czech Republic, Estonia, Finland, Germany, Latvia, the Netherlands, and the United Kingdom; along with the Swedish International Development Agency (SIDA) and the United States Department of State. DDP operates in a manner that is independent from its donors and is managed by the Humanist Institute for Development Co-operation (Hivos), a non-profit organisation headquartered in the Netherlands that provides funding and implements programmes to innovate for social change worldwide.

Initially conceived as a regranting mechanism focused on provision of urgent support to HRDs suffering from digital attacks, threats, or emergencies, DDP's programme has evolved in correspondence with the needs of these HRDs. Lessons learned from the initial implementation of this programme made clear that support in the form of funding was not sufficient in and of itself to respond in an effective way to emergencies. As a result, emergency response is now complemented and supported by a holistic programme of activities which includes sustainable responses to threats, facilitation and community building within the broader ecosystem of support to HRDs under digital threat. This holistic and community-focused approach aims to ensure a broader reach and more sustainable, systematic response to the equally systematic threats facing HRDs and Internet freedom more broadly in the current context.

DDP's Vision

An open internet, free from threats to expression, association, assembly, privacy and other fundamental rights, specifically in repressive and transitional environments.

DDP's Mission

To provide a holistic response to digital threats and create resilient and sustainable networks of support to human rights defenders. To this end, DDP provides emergency response and sustainable protection funding; strengthens rapid responders and local protection networks and capacities, and contributes to long-term organisational safety through Digital Integrity Fellowships.

DDP's Principles

A rights-based and people-centred approach is fundamental to DDP's work. Our core values are:

Do-No-Harm:

In all our interventions, DDP seeks to contribute towards unification and collaboration and decrease the potential for conflict.

Holistic understanding:

we understand digital threats as part of a complex pattern of violence against HRDs, linked closely to attacks on their freedom, and their physical and psychological integrity. Attacks are never purely digital, and neither is DDP's response.

Human rights and Internet freedom:

working with donors, partners, consultants and grantees committed to universal human rights.

Inclusivity & Diversity:

including a culture-sensitive, gender-sensitive and intersectional understanding in our analysis and support.

Mentorship & Partnership:

developing partnerships with grantees on an equal footing.

Not claiming, but facilitating:

encouraging individuals, organisations and networks to have and take ownership of their own interventions and activities.

Trust & Confidentiality:

establishing and maintaining trust with partners is central to DDP's work.

Quality & Expertise:

developing and supporting high-quality, trustable and sustainable responses to digital threats.

Who we work with

Human Rights Defenders under threat

DDP supports human rights defenders - including activists (who may or may not self-identify as HRDs), bloggers, civil society organisations, journalists, and other users of Information and Communications Technologies to promote and defend human rights, whether voluntarily or professionally, individually or as part of organisations, collectives or communities - under digital threat in repressive and transitional environments.

DDP will mainstream a gender equality and diversity perspective in our programmes and key activities, acknowledging that digital threats can affect people differently and that gender and sexual orientation are a key factor in this.

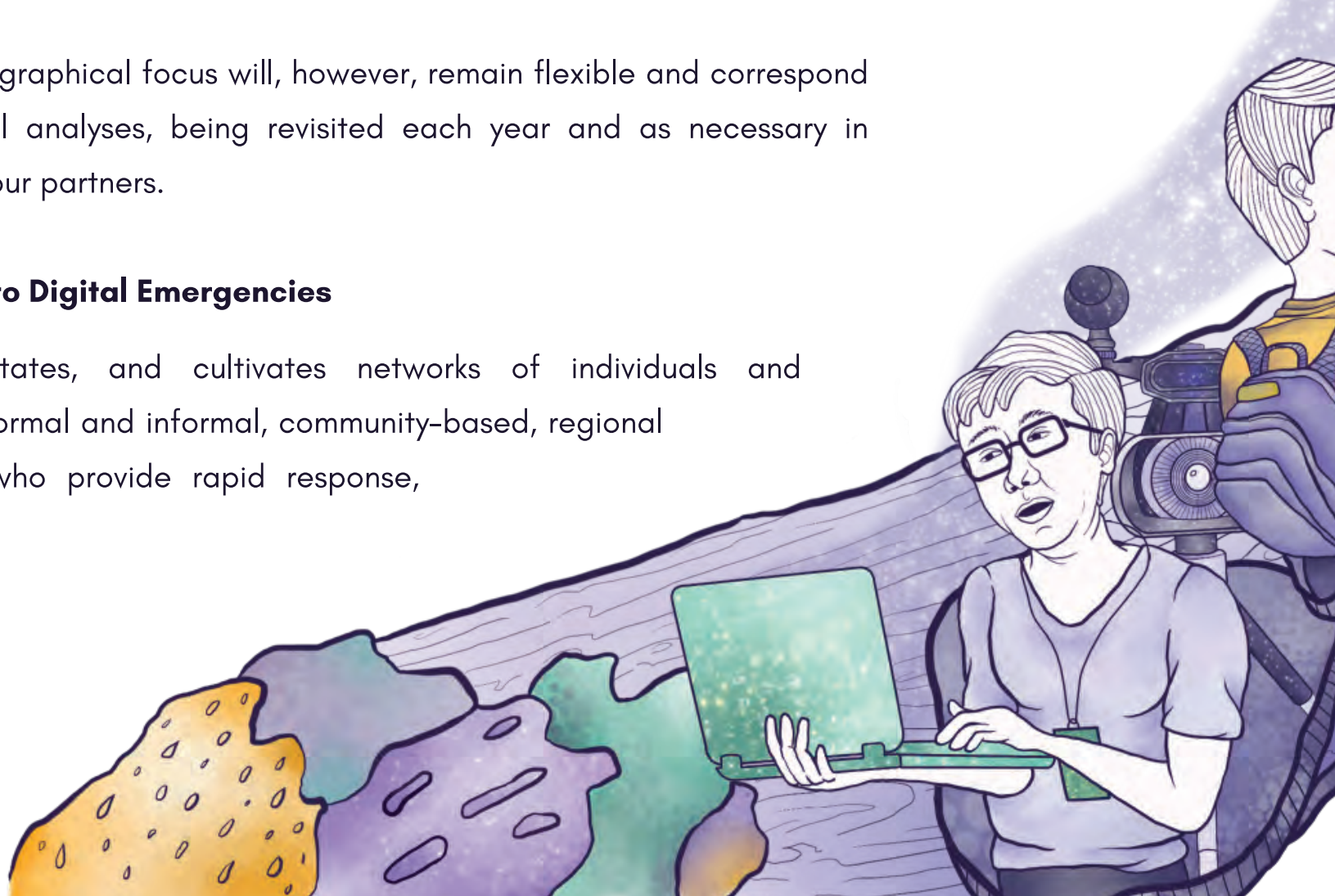
The fast changing nature of digital threats requires us to stay flexible and offer a programme of support that responds to the needs of the field. At the moment of writing this strategy (Q1 of 2019), informed by our 2018 participatory research, we will place a particular emphasis on:

- actors that collect, interpret and make data available for the broader public (including artists, bloggers, journalists and their sources, election monitors and those monitoring Internet shutdowns);
- environmental, indigenous, and land rights defenders;
- LGBTQI+ communities and those who promote and defend their rights;
- women and gender rights defenders and groups.

Our thematic and geographical focus will, however, remain flexible and correspond to ongoing contextual analyses, being revisited each year and as necessary in correspondence with our partners.

Holistic Responders to Digital Emergencies

DDP supports, facilitates, and cultivates networks of individuals and organisations - both formal and informal, community-based, regional and international - who provide rapid response,



accompaniment, advice and tools to HRDs under digital threat. This group includes those who offer diverse forms of support including legal advice, physical security support, and psychosocial accompaniment and training. This focus supports the sustainability and expands the reach of DDP's support.

II. Context and Lessons Learned

Process

Our strategy for 2020-2023 has been developed in consultation with past, present and potential beneficiaries of our work, our donors, our partners and collaborators from the previous strategic period, the DDP team itself and peers from within Hivos. Key inputs for its development included:

- An interim evaluation carried out in 2017 by Kaleidos research in which DDP donors, partners, beneficiaries and potential beneficiaries in three countries (Mexico, Uganda and Russia) were interviewed, and a number of recommendations were made for the improvement of DDP's strategy, programmes and operations;

- Participatory research with DDP staff, partners, collaborators and HRDs carried out by The Engine Room[(1)] in 2018. DDP staff and HRDs from Latin America, south-east Asia and sub-Saharan Africa were interviewed, took part in participatory focus groups, and desk research was carried out, on the basis of which a number of opportunity areas and strategic recommendations were identified;

- A participatory workshop facilitated by Confabium and attended by partners and collaborators in January 2019, at which participants carried out community-building activities, participative context analysis, identification of key topics on which to collaborate in the coming strategic period, and fleshed out possible directions that could be taken with regard to these.

We are grateful to all those who have participated in this process for their invaluable insight which has shaped our strategy for the coming years, and will no doubt continue to do so.

The context in which DDP operates

The context in which DDP will operate in the coming four years is one characterised by increasing threats to Internet freedom and human rights as well as those who seek to promote and protect them. Some of the key trends identified by DDP and our partners and which have informed our strategy for 2020-2023 are explored below.

---

(1) https://www.theengineroom.org/

Criminalisation and attacks against human rights defenders

DDP is operating in a global environment in which the space for human rights and human rights defenders, both online and offline, is shrinking due to a series of economic, environmental, legal, political, social, and technological developments.

Human rights and their universality in particular are being questioned and criticised more fundamentally at a global level than in previous years, including by actors who have traditionally promoted them.

Totalitarian, authoritarian or regressive regimes have tightened their grip on power in a number of influential countries including Brazil, China, India, the Philippines, Russia and Turkey, and there has been a notable shift to the political right which has also often come clad in an anti-rights discourse in North America as well as parts of the European Union.

In this context, HRDs are increasingly stigmatised and criminalised, being presented as radical, or targeted through the abuse of anti-terror and anti-drug-trafficking legislation. A tightening of administrative laws has also been observed, making it more difficult for non-governmental organisations to register or carry out their activities lawfully - this has, in turn, facilitated an increase in administrative harassment against HRDs.

Killings of human rights defenders remain widespread, and in this regard, land and indigenous rights defenders are among those most commonly targeted. Given the current environmental challenges which are in turn giving rise to further humanitarian catastrophes, the work of environmental and land rights defenders remains of paramount importance to the broader human rights movement(s) and humanity in general.[(2)]

There has also been an increase in the stigmatisation of philanthropy more broadly, presented by anti-rights actors as strengthening a malign liberal movement. This has in part precipitated a reduction in the funds made available for some human rights work.

Increasing surveillance and crackdowns on Internet freedom

These political developments have been accompanied, and in part facilitated, by a series of worrying

(2) See Front Line Defenders, Annual Report 2017 https://www.frontlinedefenders.org/sites/default/files/annual_report_digital.pdf and the International Center for Not-for-Profit Law, "Effective Donor Responses to the problem of Closing Civic Space" http://www.icnl.org/news/2018/Effective%20donor%20responses%20FINAL%201%20May%202018.pdf

trends regarding Internet freedom, freedom of assembly, expression, and association, and the right to privacy online.

In spite of the Snowden revelations and the now widespread public knowledge of surveillance programmes and their unlawful use against civil society, generalised surveillance remains the trend globally. New technologies, such as those based on artificial intelligence (AI) and machine learning (e.g. facial recognition), are being developed and implemented by States without due consideration to ensure their adherence to human rights standards, and there are already worrying examples of their employment against civil society in Europe and beyond.[(3)]

Targeted surveillance of HRDs, journalists and marginalised communities is widespread, including through the use of sophisticated spyware which is commonly exported to authoritarian countries.[(4)] At the same time, raids and confiscation of computers and other equipment from HRDs remain commonplace, often granting State authorities or non-State actors access to sensitive information used later to facilitate further attacks against them.

Blocking, censorship and Internet shutdowns remain commonplace during times of elections or civil unrest, despite their establishment as contrary to international law. Civil society remains under-resourced to deal with such threats in a coherent and effective manner.

Online harassment, defamation campaigns, and trolling of HRDs and marginalised communities continues to spread as the Internet remains a central tool for advocacy and impacting the public discourse. Such attacks enable and facilitate 'offline' violence against HRDs, as well as having a significant potential for psychological harm.

The infrastructure of the Internet itself is also undergoing worrying changes. There is an observable trend towards the creation of national "walled gardens", whereby citizens are denied access to the open Internet in favour of nationally-managed 'intranets' which are characterised by surveillance and censorship. Furthermore, the Internet 'backbone' - the cables which transfer data between countries and Internet Exchange Points - are also changing hands, away from telecommunications companies and

---

(3) See for example the deployment of facial recognition technology by police forces in England and Wales as detailed by Liberty: https://www.libertyhumanrights.org.uk/resist-facial-recognition

(4) See for example the Citizen Lab "Hide and Seek" series: https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

(5) See "Internet Drift: How the Internet is likely to splinter and fracture" by Steve Song https://digitalfreedomfund.org/internet-drift-how-the-internet-is-likely-to-splinter-and-fracture/

towards large multinational companies such as Facebook, Google and Microsoft[5], all of whom have been notable for their collaboration with authoritarian regimes in restricting Internet freedom at given times, and whose business models are inherently problematic from a human rights perspective, being based in large part on the collection, analysis and sale of personal user data which fuels surveillance and data discrimination. Forced user interaction with the data-driven and surveillance-friendly business models of these companies will negatively impact their ability to exercise their rights to privacy and free expression online; it will also likely increase the phenomenon of "data discrimination", in which marginalised communities will be further socially excluded as a result of the functioning of opaque algorithmic processes.

Access to tools for data protection and free expression

Recent years have seen the spread of tools and protocols which increase the ease with which HRDs can protect their information, evade censorship and communicate securely online - a demonstrative example being WhatsApp's implementation of end-to-end encryption in 2016, which was followed by a number of other popular applications such as Rakuten Viber.

This development stands in contrast, however, to the trend of diminishing user control over and devices, which leaves them vulnerable to backdoors and reduces their opportunities for the use of alternative, more secure software. This has in turn spurred a movement which articulates and promotes the right to repair, also arising from the problems associated with increasing e-waste and its environmental impact.

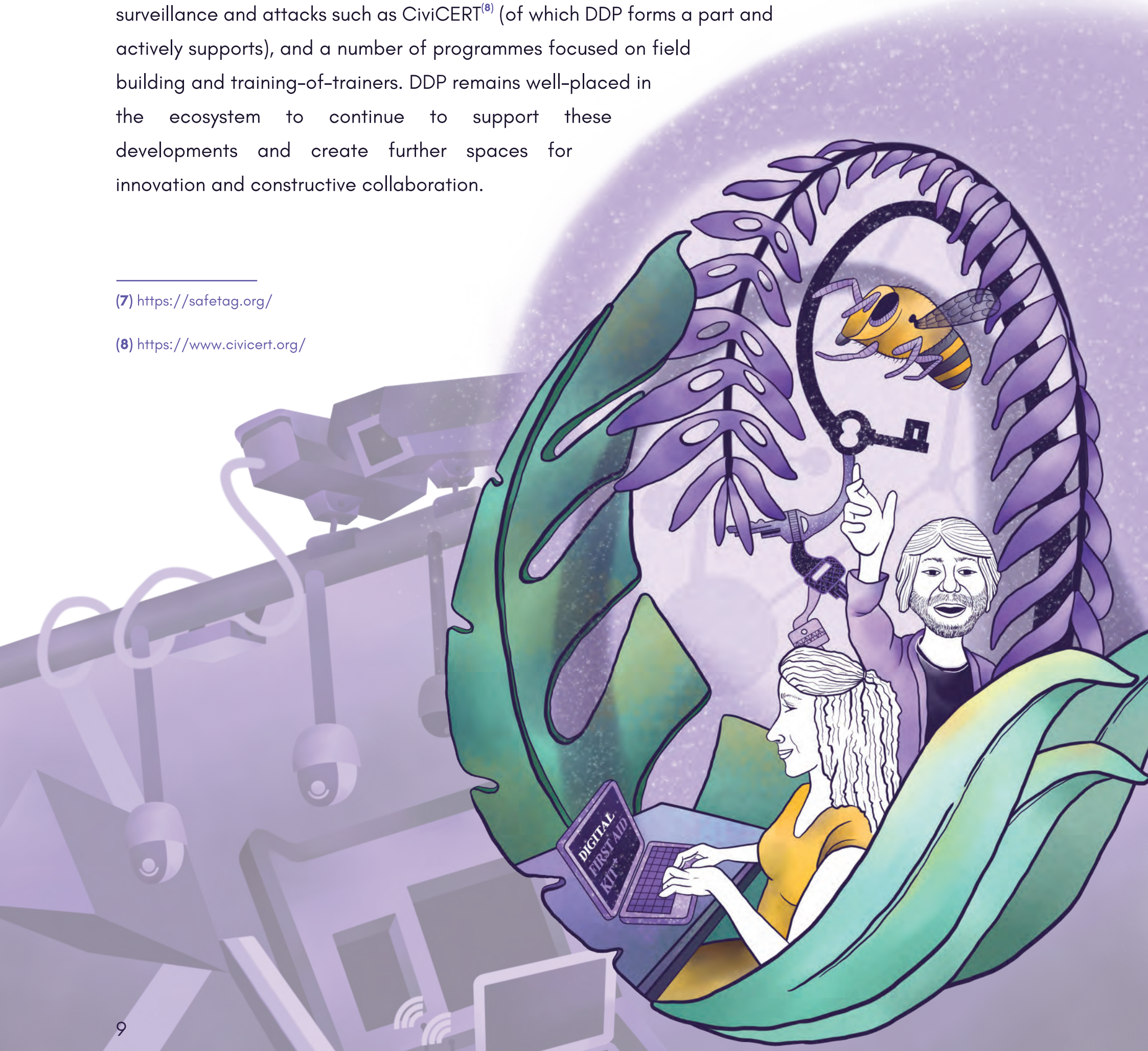
Strengthening and diversity of the HRD protection field

Recent years have seen several positive developments in the broader ecosystem to which the DDP is connected - including those of security and protection of HRDs, freedom of expression, promotion of the right to privacy, and Internet freedom, among others. These developments include the establishment of more programmes and organisations dedicated to the protection of HRDs, including with a focus on digital security. An overall trend has been increasing recognition of the need for a holistic approach - considering the intersection of the psychosocial, legal, physical, and digital aspects in analysing political violence against HRDs, and in the construction of protection strategies. There has also been increased recognition of the value of a gender-sensitive and intersectional understanding of the same. The merits of accompaniment and coaching alongside trainings and workshops, and a somewhat more critical approach to one-off trainings has also been broadly acknowledged. DDP, including its Fellows, has actively promoted and supported these developments in the previous strategic period[6], and aims to

(6) An example in this regard is the development of the Open Technology Fund Digital Integrity Fellowship based on the model first established by DDP in 2015.

continue to deepen integration of holistic and gender/intersectional perspectives in all aspects of its work. DDP is well positioned to contribute positively in this regard to the broader community, and intends to facilitate further contact and collaboration between interdisciplinary groups focused on protection of HRDs, as well as promoting resilience and building awareness and capacities within the rapid responders networks.

With regard to digital securitay and Internet freedom more specifically, there have been positive developments in the establishment and rollout of security auditing frameworks for civil society organisations, such as SAFETAG[7], and research and support activities related to targeted surveillance and attacks such as CiviCERT[8] (of which DDP forms a part and actively supports), and a number of programmes focused on field building and training-of-trainers. DDP remains well-placed in the ecosystem to continue to support these developments and create further spaces for innovation and constructive collaboration.



(7) https://safetag.org/

(8) https://www.civicert.org/

Key lessons learned

Based on the above trends and following on from our interim evaluations and participatory engagements with beneficiaries and partner organisations, DDP has identified a number of lessons which will guide the development and implementation of our activities in the coming strategy. Some of the most salient guiding principles include:

- **Consolidation and flexibility:** The flexibility and innovation which characterises DDP's mandate and approach to activities is valued by our collaborators, allowing us to fill important gaps and respond creatively to needs as they arise. We will seek to maintain this characteristic in the coming years, while also focusing and consolidating our work in order to ensure limited resources are well used, and that useful lessons can be learned from innovative programmes such as the Digital Integrity Fellowship and strengthening of regional Rapid Responders Networks.

- **Facilitate actively in the global Rapid Response Network (Rarenet) and regional Rapid Responders Networks:** 'Rarenet'[9] is a global network composed of diverse actors that provide emergency response and support to individuals or organisations facing digital threats. The aim of the network is to enable spaces for trust building, threat- and knowledge-sharing for a better coordination of digital emergency responses. It also facilitates support and solidarity building among the individual members and the organisations they represent. Rarenet members work with a diverse group of trainers and digital/holistic security experts embedded in different regional contexts and local communities.

(**9**) https://www.rarenet.org/

Further to this, DDP has supported the creation and maintenance of similar rapid responders networks at regional level in the Former Soviet Union (FSU), Latin America, and the Middle East & North Africa (MENA) regions, and will continue to do so in the coming strategic period. DDP aims to create further bridges among regional rapid responders networks (RRN), supporting more exchange between Rarenet and regional RRN members. In order to improve RRNs' outreach and impact, DDP will clarify entrance points to these networks for those that could take advantage of their support, and enable documentation of processes in order to facilitate the possibility for local initiatives to set up specific rapid responders networks that fit their needs. Finally, DDP will start investigating the need expressed by different RRNs to provide more opportunities for tailored training-of-trainers and training curricula that are specifically oriented towards rapid responders and take into account their needs, threats and capacities. Shaping more capacity building among RRN will be achieved through partnership with all DDP partners and the DIF.

- **Strengthen Gender Equality and Diversity Inclusion (GEDI):** DDP will mainstream a gender equality and diversity perspective in our programme and key activities, in line with the Hivos Gender Equality and Diversity Inclusion (GEDI) strategy[10]. We do this by acknowledging that our activities can affect people differently and that gender and sexual orientation are a key factor in this. Women and men, as well as people who are gender non-binary, have different perspectives, needs, roles and resources, and class, race, ethnicity, disability and age may reinforce these differences. Therefore, DDP will incorporate an assessment of the implications of our interventions for different people and addresses these differences and other power structures that create inequality for individuals and communities with regard to their access to security and protection.

(10) The Gender Equality and Diversity Inclusion Strategy emphasizes gender as both a cross-cutting theme in Hivos' work and the focus of distinct programming, research and advocacy. It ensures that Hivos continues to support programs that consistently address gender inequalities, acknowledge diversity and contribute to building a body of staff that represents the societies we serve. https://www.hivos.org/who-we-are/our-organization/integrity/

- **Learning actively and sharing lessons:** As an innovator and facilitator of dialogue and the development of best practices in the ecosystem, DDP is now well placed to establish mechanisms for learning from our work, and share these along with the lessons which come out of it, with our partner organisations and the broader ecosystem.

Simplified and improved outreach: DDP's communication regarding its grants and other kinds of support offered will be simplified, clarified, and made easier to access.

Strengthening of local and regional capacities: Attacks on HRDs and crackdowns on Internet freedom often require responses which are informed by deep knowledge of the local contexts in which they take place. DDP therefore seeks to strengthen regional and locally-embedded Fellows, rapid responder networks, Internet freedom and digital security initiatives.

Continue with the holistic approach: The holistic approach to digital threats adopted by DDP in its activities has been well received and continues to be validated more broadly in the field of HRD protection. DDP will continue to engage with allies – old and new – to deepen and improve this nascent approach.

- **Increasing transparency:** DDP will make non-confidential information on our activities more easily available to a wider public. We will implement a section on DDP site resuming our outcomes and creating a public version of our annual reports. Our efforts to increase transparency will be undertaken without undermining the confidentiality necessary to our work.

1. Provide timely, flexible and holistic emergency response resources to reduce the impact or risk of digital attacks against human rights defenders;

III. Theory of change

DDP believes that human rights defenders and activists, and the work they carry out, are of fundamental importance in promoting and protecting human rights globally, and that a free and open Internet is equally important in facilitating and potentiating their work.

Our overall objective for the coming strategic period is for human rights defenders in repressive and transitional environments to access improved capacities and networks so that they can continue their work despite digital threats.

We have three strategic goals which we believe will contribute towards this objective:

2. Strengthen awareness and capacities for sustainable and effective responses to digital threats among human rights defenders at risk;

3. Develop and maintain accessible, collaborative, resilient and responsive networks of expertise and support for human rights defenders under digital threat.

Goals and activities

In order to achieve the aforementioned goals and our overall objective, DDP will employ three areas of work:

1. Incident Emergency Response,

2. Sustainable Protection Support, and

3. Facilitation and Community Building.

Each area of work has at least one key activity, and is also supported by **transversal activities** that contribute to two or more goals, all of which are explored further below.

1. Incident Emergency Response

Goal: Provide timely, flexible and holistic emergency response resources to reduce the impact or risk of digital attacks against human rights defenders.

In order to provide timely, flexible and holistic emergency response resources to reduce the impact or risk of digital attacks against human rights defenders, DDP will continue to supply incident emergency funding in the most strategic manner possible, and promote collaboration with and among our allies to ensure emergency cases receive the most appropriate and holistic response possible.

Key activity 1: Incident Emergency Funding

DDP will continue and improve our provision of Incident Emergency Funding (IEF) grants of up to €10,000 in response to requests from HRDs in imminent risk, or in the aftermath of digital attacks.

In 2020-2023, DDP will support approximately 70 HRD individuals/organisations/networks with Incident Emergency Funding through our basket fund. A majority of IEF grants will be granted to priority groups (according to geographical and thematic focus) defined in collaboration with partners each year or as necessary in accordance with context. Criteria and protocols for defining priority groups will be developed in collaboration with partners in 2019. Given DDP's orientation and position in the field, we will also seek to prioritise lesser-known, underprivileged groups who are at risk of 'falling through the net' and may find it difficult to receive support from other organisations.

This funding will be used to cover hardware, software, accompaniment, coaching and training related to digital security, as well as related aspects of security and protection. Where necessary and possible, IEF will be made available to cover non-digital aspects, including through psychosocial and physical security support, which may also be necessary in light of, or in the aftermath of, digital attacks.

DDP will regularly communicate and plan with partner organisations to prepare for, and be able to respond in a collaborative manner to, local and regional high-risk events - such as elections, mass protest movements or peacebuilding initiatives - in a collaborative manner.

DDP will develop and implement participative methods of evaluating our Incident Emergency Funding,

which will be regularly refined in order to ensure it responds to the needs of HRDs under digital attack and occupies a useful space within the ecosystem of support. As noted above, we will communicate more regularly about the funding provided and its impacts, through reporting as well as informally through blogs and social media.

Key activity 2: Facilitating referrals

Due to limitations arising from funding, organisational mandates, or internal policies, it is often the case that organisations in our ecosystem are unable to respond positively to requests for support by HRDs under digital threat and as a result, these cases often require onward referral to other organisations. As a trusted partner at the intersection of several communities, DDP is in a strong position to facilitate referrals of requests and needs of HRDs under digital threat within the community. DDP will maintain and update a secure referral database, established in 2019, composed of trusted individuals and organisations along with the types of support they offer, in order to facilitate referrals between and among them on request.

Key activity 3: Digital First Aid Kit and other resources

DDP will continue to guide and facilitate the maintenance of the Digital First Aid Kit (DFAK)[11], which will help rapid responders, digital security trainers, and tech-savvy activists to better protect themselves and the communities they support against the most common types of digital threats.
Further to the above and pending funding, in collaboration with others, DDP will also explore the possibility of contributing to the maintenance of community learning resources which are valuable but currently unmaintained.

(11) https://rarenet.gitlab.io/dfak/en/index.html

2. Sustainable Protection Support

Goal: Strengthen awareness and capacities for building sustainable and effective responses to digital threats among human rights defenders at risk.

Seven years into DDP's existence, we have recognised that while emergency response is important and beneficial, it does not go far enough in coherently addressing the impact of digital threats faced by HRDs in the context in which we are operating. Organisations and networks working in particularly high-risk contexts need to build sustainable capacities for longer-term resilience in order to continue their work in the face of hostile contexts, thereby reducing the need for reactive emergency support.

Key activity 4: Sustainable Protection Funding

In the 2020-2023 period, we will continue to make grants of Sustainable Protection Funding (SPF) to human rights organisations and emergency responders in order to improve the sustainability of their work in high-risk environments. SPF grants range from between €10,000 and €50,000 over a one-year period, and are available for organisations or networks (rather than individuals). This funding can be used to cover improvements in an organisational digital security apparatus (infrastructure, trainings), tests/research of specific threats, and temporary support needed to mitigate a specific digital emergency situation, among other needs. Psychosocial and physical security support can also be covered by SPF.

This activity is demand driven, with organisations in imminent risk or in the aftermath of digital threats reaching out to DDP for support. As with Incident Emergency Funding, DDP vets SPF requests via our trusted network and assesses these requests based on a variety of criteria, such as urgency of the digital threat, quality of the application, impact of the proposed intervention and sustainability of activities. We aim to have most of our SPF support reach our priority groups.

In 2020-2023, DDP aims to support approximately 32 organisations/networks with Sustainable Protection Funding through our basket fund. Of these, we aim for approximately 20 be granted to priority groups defined in accordance with the criteria and protocol to be developed as mentioned above.

Throughout the coming strategic period, participative research will be carried out to establish the impact of sustainable protection funding on the safety and effectiveness of its recipients (see Transversal Activity 2).

Key Activity 5: Digital Integrity Fellowship

The Digital Integrity Fellowship (DIF), which began in 2015, was developed as a response to the problematic trend of "box-checking" digital security trainings being carried out with little scope for follow-up or adjustment of the content to the beneficiaries in question or their context-specific needs. The DIF programme provides organisations, collectives, and networks with a tailored programme of accompaniment from at least one DIF Fellow for between six and 18 months. The DIF programme supports their awareness of digital security issues, the development of effective and resilient practices for digital security, and a positive contribution to the overall protection and well-being of the collective. Where necessary, Fellows will collaborate with DDP partners, rapid responders and Hivos Regional Hubs to ensure a tailored and holistic approach is taken, and resources available are taken advantage of.

The four years since the DIF began have seen it grow into a cohort of experts primarily embedded in communities, while the need was also recognised for fellows among the cohort who provide transversal support, such as in IT architecture or knowledge management. This flexibility of the model will continue, with an emphasis on a cohort of Fellows embedded in local contexts, movements and/or organisations. The cohort of Fellows will be renewed on an ongoing basis.

The Fellowship model supports consultant experts on digital security, otherwise potentially in danger of isolation, under-funding and a cycle of 'training-to-training' work, to work together in a transnational and multi-disciplinary community, learning from one another and building skills and networks, while facilitating dynamic processes of change in the organisations they support with a holistic methodology. Fellows work with internal focal points within organisations and networks, with the aim of ensuring that the collective capacities for sustainable responses to digital risk are strengthened. Furthermore, DDP arranges for Fellows and focal points from across regions to meet and network in the context of international human rights events and conferences in order to facilitate the growth of their networks in a manner consistent with our holistic approach.

Where possible, Fellows can be deployed to offer support in the aftermath of emergency situations which are communicated to DDP.

In the 2020-2023 period, DDP aims to support a consistent cohort of six to eight Fellows along with Trainee Fellows in three regions (see Mentorship and Field Building, Transversal Activity 3). The methodology employed and learnings from the first four years of the Fellowship will be shared with the broader community through the DIF Manual which will be published and outreached in 2019.

This will be accompanied by an ongoing process of participative research for deeper critical learning and evaluation of the model, and how it evolves in the distinct contexts in which it is employed.

In correspondence with the Mentorship and Field Building Project (see Transversal Activity 3) the DIF model will continue to develop towards a strengthening of local and regional capacities, while cohorts will remain connected and in contact in order to facilitate learning and sharing of best practices.

3. Facilitation and Community Building

Goal: Develop and maintain accessible, collaborative, resilient and responsive networks of expertise and support for human rights defenders under digital threat.

A healthy ecosystem of support, characterised by collaboration and trust across organisations, regions, and areas of expertise, will help to ensure that HRDs under digital threat can more easily access the support they need in moments of high risk or digital attacks. This will also help to overcome some of the challenges posed by limitations on funding, mandates, expertise or resources on organisations. Support will also be more effective when it comes from a source which has deep contextual knowledge of the situations facing HRDs; this increases trust, accuracy of analyses, and adequacy of the support given. To this end, DDP will continue to support and facilitate collaboration and community building in the ecosystem, both globally and locally.

To date, this area of work has been represented primarily by DDP's facilitative and supportive work in the global Rapid Response Network (Rarenet), and regional Rapid Responders Networks (RRNs), which has received positive feedback and inspired calls for DDP to take a more active facilitative role.

In the coming strategic period, DDP will reach out to groups currently underrepresented in the ecosystem (such as land rights defenders, sex workers, and others) in order to ensure that it benefits from a diversity of actors, and in order to facilitate support to the most heavily targeted and underprivileged groups.

This area of work is also key in achieving a "multiplier-effect", increasing sustainable and context-specific capacities for responding to digital threats and avoiding centralisation of expertise in the field.

Key activity 6: Strengthening the global Rarenet

DDP will continue to financially support and facilitate meetings and trainings for members of the global *Rarenet*, in accordance with the needs of the community. We will also facilitate meetings for members of

the *Rarenet* at international events such as the Internet Freedom Festival and RightsCon, among other meetings deemed useful, such as those necessary to work on shared resources.

DDP will seek to expand membership of the *Rarenet* to include further individuals and organisations who can contribute legal, physical security and psychosocial support to HRDs under digital threat, as well as the network itself when necessary, thus supporting further development of a holistic approach.

DDP is also a member of CiviCERT, the Computer Incident Response Center for Civil Society. CiviCERT is an umbrella organisation formed by Internet content and service providers, NGOs and individuals that contribute part of their time and resources to the community in order to globally improve the security awareness of civil society. CiviCERT assists civil society organisations in handling the technical and organisational aspects of incidents in connection with other Computer Security Incident Response Team (CSIRT). In particular, it provides assistance or advice with regard to incident triage, incident coordination, incident resolution and proactive services such as malware analysis, legal advice, security training for civil society and detection of network interference. We will continue supporting this initiative and enable more organisations to join in the coming strategic period.

Key activity 7: Facilitating development of regional Rapid Responders Networks

Consistent with our ongoing focus on strengthening local and regional capacities, DDP will support the further development and maintenance of regional Rapid Responders Networks in the 2020-2023 period.

The approach to this will not be "one-size-fits-all", nor seek to impose the model from one region onto another, but rather will be consistent with the regional context and the subsequent needs of HRDs and the organisations and individuals supporting them. Furthermore, in a manner consistent with our holistic approach, we will encourage these networks to adopt a multidisciplinary understanding of digital threats against HRDs, including among their members those offering digital security training, coaching, or accompaniment; technological infrastructure; organisational security support; legal support; mediation, and psychosocial support, etc., and strongly encouraging a gender-justice and intersectional approach.

DDP continues to support the networks in the FSU, Latin America, and MENA regions, and is looking into the establishment of new networks in Southeast Asia and East Africa. Working with regional coordinating partners, DDP will work to promote capacity, trust and community building among these organisations and individuals, in accordance with necessities, through supporting conferences, meetings, trainings, intervision or other activities among RRN participants.

Aware of the potential harm caused by bringing resources to environments which are occasionally characterised by a damaged social fabric, DDP will work with a Do-No-Harm (DNH) approach[(12)], seeking to strengthen existing networks rather than replace them, and contribute towards increased collaboration and unification of the human rights, digital rights and Internet freedom communities in each region.

Key activity 8: Supporting holistic approaches

DDP has been a strong proponent of, and adherent to, the holistic approach to security and protection of HRDs. While a number of our partners and collaborators share this approach, there are currently few if any regular spaces created for exchange and deepening on the meaning of the approach, and building the necessary knowledge, contacts and skills in order to translate this into effective programmatic support. In the coming strategic period, DDP will create regular spaces for this exchange, dialogue, and learning, both in order to facilitate the adoption of holistic approaches by our partners in the global and regional networks, and to contribute to the sustainability and security of ecosystem itself.

In connection to this, DDP will explore the establishment of minimum necessary professional standards on psychological well-being for individuals in our networks carrying out emergency response work and working with HRDs at risk, and seek to establish contact with organisations and networks which can offer support in this regard.

Additional activities

IIn accordance with needs articulated by allies and collaborators as well as our external reviews and research, DDP will continue to actively promote and facilitate collaboration between actors with complimentary expertise, and reach out to other communities with which we have to date had less contact. We will also continue to engage actively and productively with our donors and other allies including the diplomatic corps in order to facilitate connections, share knowledge and build capacities where necessary.

(12) The Do-No-Harm (DNH) approach, developed by CDA collaborative, aids those planning development interventions to so in a conflict-sensitive manner, identifying and controlling for the potential negative effects of the intervention. See https://www.cdacollaborative.org/what-we-do/conflict-sensitivity/

Transversal activities

All of the aforementioned goals are supported by a further set of transversal activities: Partnership Funding, the Mentorship and Field Building Project, Learning and Promotion of Best Practices.

Transversal activity 1: Partnership Funding

DDP offers Partnership Funding to support programmes of work which complement that of DDP and which we consider to be of particular strategic value.

Partnership Funding ranges from €10,000 to €200,000 per year and can be re-applied for on an annual basis. Partnership Funding supports activities of organisations in the ecosystem which are strongly complementary of DDP's activities, strategic, effective, consistent with our values, and contribute to our shared goals and overall objective.

Partnership Funding has previously included, for example, supporting a team of digital security experts to carry out accompaniment, assessment, coaching and training for organisations in several regions; provision of legal support to HRDs and journalists under digital threat and strategic litigation on digital rights; and provision of secure digital infrastructure to human rights defenders, organisations, collectives and movements.

In the 2020-2023 strategic period, DDP will continue to offer Partnership Funding, based on a call for applications and criteria which will be developed in consultation with collaborators from the ecosystem in 2019. It is envisaged that we will support between three and five Partners per year.

General guiding characteristics of projects or organisations which will be prioritised for Partnership Funding will include:

- *Global Scope, Local Focus:* DDP will seek to support activities which are not limited to a particular country or region, but are ideally developed and implemented in multiple regions and/or globally. However, a corollary condition of this is that the activities in question should aim to strengthen local capacities, draw on local knowledge and networks, and embed expertise within organisations, collectives and movements.

- *Holistic and complementary:* DDP will seek to support activities which are complementary to our digital focus and contribute to our goals with skills and knowledge from other disciplines, including organisational security and protection, psychosocial support, or legal support.

Transversal activity 2: Mentorship and Field Building Project

Building on the success of the DIF project to date, DDP will support the spread of this model in the coming strategic period through the development of three regional communities of individuals and organisations who can offer this type of accompaniment to human rights organisations and networks.

DDP's Project will be prototyped in south-east Asia in 2019, and lessons learned will be implemented in subsequent phases of the project (Latin America and sub-Saharan Africa) in 2020-2023.

In each region, DDP will establish networks of Trainee Fellows who will receive training and mentorship from experienced digital and holistic security experts in order to carry out accompaniment following the DIF model with human rights organisations, activist networks and collectives. An initial Trainee Fellow cohort in each region will undergo a two-week training and, subsequent to this, carry out Trainee Fellowships accompanying one human rights organisation to improve their digital and overall security for three months. During this time, the Trainee Fellows will receive mentorship from two regional mentors (a team of which will also be trained and supported beginning in 2019) as well as benefitting from intervision within the cohort while carrying out their accompaniments. The intervision and exchange between regional Trainee Fellows and mentors will be supported by the development of an online platform for knowledge management and exchange, as well as "linking and learning" events which will be organised on a yearly basis. The project will aim to build on and strengthen existing local capacities and resources; the form which accompaniment takes will be adapted to the needs and contexts in question.

As a part of this process, DDP will reach out to others who are interested to develop, implement and refine common monitoring and evaluation frameworks informed by critical social sciences to facilitate improvements in common or similar activities across the communities in which we operate. DDP will facilitate spaces for interactive and participatory research with partners and collaborators working towards the same goals in order to facilitate comparative analysis, debate, and development of best practices.

The results of all of the above activities will be shared with the broader ecosystem through a communication strategy which will be developed in 2019, and will include informal outreach through blogs, video conferences, storytelling and case studies, as well as contributions to academic and practice-based journals, coordination of global linking and learning meetings, and participation in conferences on human rights, Internet freedom, and protection of human rights defenders among others.

With a view to supporting a rotund response to digital threats, this communication strategy will include outreach to organisations carrying out lobby and advocacy on issues related to digital rights and HRD protection, who may benefit from data gathered by DDP concerning digital threats.

Sustaining and Developing DDP

The programmes and human resources of DDP have expanded significantly since our establishment, now boasting seven dedicated staff members, of which two are working remotely. Further growth in staff, including remotely-based colleagues, is expected in the coming strategy period, particularly in the context of the Mentorship and Field Building Project: we envisage by the end of the coming strategy period having at least one dedicated staff member in each of Hivos' regional Hubs. DDP is aware that this growth, if it is to be well managed, implies a consideration of the structures necessary to remain as well organised as necessary, and as flexible as possible, and our needs in this regard will be explored in 2019 with a view to establishing the necessary changes in this regard.

IV. Key Terms

- **Digital Threat:** Actions or intentions of malicious actors to constrict or otherwise negatively impact the work, physical or psychological well-being of others through the use of digital media or technology.

- **Ecosystem:** Refers to the multitude of activists, collectives, organisations and networks with which we share common values, goals and objectives. This includes those with a focus on digital rights, emergency response, Internet freedom, privacy rights, protection of human rights defenders, technological autonomy, and many more.

- **Holistic security:** An approach to security and protection of human rights defenders which recognises the need for, and promotes, interdisciplinary understanding of political violence and the strategies needed to reduce it. This interdisciplinarity includes, but is not limited to: 'hard' security, psychosocial approaches, legal and administrative aspects, and digital security.

- **Intersectionality:** A feminist method of analysis which seeks to visibilise overlapping forms of discrimination (such as through race, disability, ethnicity, gender identity, religion, sexual orientation, etc) and take them into account when fighting for equity, justice and human rights.

- **Repressive and Transitional Environments:** Rather than referring to a specific country, region, or set thereof, repressive and transitional environments can be found globally, wherever a movement to articulate, establish or ensure respect for universal human rights is met with political violence from those opposed to it.

- **Transversal Activities:** DDP activities which aim to contribute to all three of DDP's strategic goals.

Annex: Strengthening Gender Equality and Diversity Inclusion

Digital
Defenders
Partnership

1. Context and Purpose of this Strategy

The purpose of this strategy is to guide DDP's adoption and strengthening of a structured approach to Gender Equality and Diversity Inclusion, corresponding to the needs of HRDs, DDP's collaborators and partner organisations that work to support HRDs, and DDP internal policies, strategies and staff capacity needs.

DDP essentially adopts a feminist and intersectional approach as the epistemological basis for our analysis and the development of our internal and external programmes. That is to say, we are actively looking to make visible and ponder power relations taking place in our strategies, the way HRD and holistic responders work and how DDP relate to partners and donors. Our positioning is complemented with an approach to digital security and overall protection of HRDs, and work with other Holistic Responders, that is developed through a lens which seeks to make the various layers of structural and discursive discrimination visible. As these leads to the marginalisation and repression of people and communities based on their gender identity, sexual orientation, race, ethnicity, caste, culture, disabilities, age, or socio-economic status, among other aspects. The means by which this discrimination is realised and perpetuated are pervasive in political, economic, social, and technological structures and are relevant to DDP's work in at least the following respects that will be explored more in-depth below:

- With respect to the risks faced by Human Rights Defenders and the different ways of accessing protection and security;

- With respect to the capacities and characteristics of Holistic Responders to Digital Emergencies, and other partner organisations of DDP;

- With respect to DDP's internal operations.

Therefore, while gender orientation is a key element of this strategy - gender-based violence being a particularly pervasive issue globally - we do not intend to treat it in isolation from other forms of structural violence based on the categories mentioned above, and more.

1.1 Human Rights Defenders

A gender-justice and intersectional analysis is of fundamental importance in order for DDP to achieve its goal of responding holistically to digital threats faced by human rights defenders. First of all, it helps to understand the risks themselves that human rights defenders face: HRDs - including women, LGBTIQ people, antiracist activists, land rights defenders, and so many more - are often, through their actions, challenging deeply embedded power structures based on gender, caste, ethnicity, race, and many others. HRDs themselves often represent women and marginalised groups. As such, the violence they face is also part of a continuum of discrimination against these groups.

Adopting an intersectional approach to understanding the risks faced by HRDs, online and offline, implies that we seek to establish and visiblise the ways in which women, LGBTIQ+ people and other marginalised groups are affected by forms of violence which are otherwise invisible or overlooked. Taking into account Gender, Sexual Orientation and Race is a way to acknowledge mechanisms enabling stereotyping, exclusion and marginalisation and which result in prejudice, racism, misogyny, phobia, hate speech and gender-based violences.

The last decade we have seen a significant rise in harassment and gender-based violence against Women Human Rights Defenders (WHRD), LGTBIQ+ and cultural minorities. The increased use of the internet and media platforms have mirrored, complemented and amplified old and new forms of violence against them. These groups are too often trapped between the need, on the one hand, to use the internet as a crucial tool for their work and activism, but also for shaping and displaying their identities and culture, and, on the other hand, the obligation to constantly navigate their exposure to surveillance, harassment, censorship and judicial harassment. Online and offline gender-based violence exists in a continuum. In many cases, different violent actions and attacks overlap, creating a complex matrix of harm with solutions that can only be assessed in a multilayered approach that involves technical knowledge, legal expertise, strategic communications, psychological support and networks of support and solidarity.

Because of this specific challenges and the sexualised, gendered and racist aspects of digital attacks oriented at women, LGTBIQ+ and other marginalised groups, over the past years DDP has supported individuals, groups and initiatives tackling these issues through Funding, the Digital Integrity Fellowship, Rapid Responder Networks and other Linking and Learning activities.

Nevertheless, DDP strives to reach out to HRDs and groups still currently underrepresented such as land rights defenders, indigenous communities, sex workers, or LGTBIQ+ located in rural areas, for instance. Because of this, this strategy aims at facilitating DDP's support to the most heavily targeted and underprivileged groups and ensure our impact in strengthening gender equality and diversity inclusion throughout its program.

While much of what DDP has done in this regard has been a result of an informal approach, we will seek through this strategy to adopt a more consistent and structured intersectional approach to our understanding of the risks faced by HRDs and the different ways they access protection and security.

1.2 Holistic Responders

DDP seeks to achieve its aims in active collaboration with a diverse set of individuals, collectives, organisations and networks worldwide, focused on digital security as well as overall protection and empowerment of HRDs, freedom of expression, promotion of the right to privacy, Internet governance and Internet freedom, among others.

Broadly reflecting, this "ecosystem" has also struggled with a lack of diversity in its makeup and a subsequent lack of nuanced understanding of the risks faced by HRDs, especially women and marginalised groups, and therefore in providing an adequate response. There has been also a lack of reflection and action to understand how some members of these support networks have been more vulnerable due to sex and gender, age, location or socioeconomic status. However, recent years have also seen several positive developments. These developments include the establishment of more research, programmes and organisations dedicated to the protection of HRDs that recognise the value of a cultural, gender-sensitive and intersectional understanding of protection and security. Some of these initiatives have also included a feminist approach to technologies by assessing their economic, political and ecological impact and how they enable mechanisms of oppression, discrimination or liberation for WHRD, LGTBIQ+ persons and other marginalised groups.

An overall trend has been the increasing development of tailored resources about hate speech and gender-based violence, and a recognition of the need for a holistic approach - considering the

intersection of the psychosocial, legal, physical, and digital aspects in analysing violences against women, LGTBIQ+ and cultural minorities, and in the construction of protection strategies. Accordingly, there has also been an increase in feminists, women and LGTBIQ+ people that are providing digital security training or rapid responses for tackling gender-based violence online and other digital emergencies. Similarly, initiatives that deal with feminist infrastructure, encompassing internet protocols to hosting and servers solutions, have grown and helped to shape an active scene that interacts and overlaps with the feminist digital security scene.

All these are very positive trends that should be taken into account for creating more equity and diversity inside the field of digital and holistic security. Nonetheless, it should also be understood that these trends are still largely localised in reduced pockets which often struggle with precarity, lack of sustainable models and/or criminalisation processes. They represent a drop of hope that should be nurtured against the global trend of technologies enabling more hate speech and gender-based violence.

We believe that the trajectory of DDP in supporting and working with different individuals, organisations and initiatives dealing with women, LGTBIQ+ and other discriminated groups can inform our strategy for strengthening Gender Equality and Diversity Inclusion in the broader DDP ecosystem. We intend to facilitate further contact and collaboration between interdisciplinary groups focused on protection of WHRDs, LGTBIQ+ and other discriminated groups, as well as promoting resilience and building awareness and capacities within our grantees, partners, rapid responders networks and Digital Integrity Fellows.

1.3 DDP's Internal Operations

The DDP core staff and our Digital Integrity Fellows are characterised by cultural diversity. This diversity is cherished and enriches both our personal and professional relationships and our work. At the time of writing, our team, including staff and fellows, is composed of 16 persons and identify predominantly as female and some also self-identify as part of the LGTBIQ+ community. However, we also recognise that various dynamics of privilege and power are always present, and are perhaps sustained by the makeup of the group itself. We recognise that in regard to the HRDs we support, we are in a position of great privilege that comes with working for an international development organisation and must act in a manner which is mindful of this dynamic.

To do so, establishing steering processes (for monitoring, budgeting, performance review processes, family/work conciliation) and analyzing how DDP targets, strategies and measures can be also viewed through a gender and diversity lens will be mainstreamed across our internal operations. As noted further below, our intention is to continue to diversify the composition of the programme through expansion of our Digital Integrity Fellowship in three regions and on the subsequent recruitment of new staff members in each geography to support them. Of special importance for the field building project, we will shape decision making processes that take gender and diversity into account. Decisions should be informed by an intersectional analysis, and decision makers should be gender-balanced and diverse.

2. Strategy Rationale

Departing from the specific challenges detailed in the above context, DDP will mainstream a gender equality and diversity perspective in our internal operations, programmes and key activities in line with the Hivos Gender Equality and Diversity Inclusion (GEDI) strategy and will complement it with an analysis of lessons learned in the gender and tech field. Our main targets for this strategy are DDP team, fellows, partners, grantees, rapid responders and funders.

We do this by acknowledging that our activities can affect people differently and that race, gender, sexual orientation, class, ethnicity, disability and age are key factors in these differences. And by acknowledging how these structures are embedded and played out in our everyday practices and in our interactions with technology, we can also honor the diversity of positioning and self-inclusion happening among our target publics in relation to protection and digital security.

Our view is that DDP's strategy should adopt a gender transformative approach to identify, tackle and remove barriers faced by women, LGTBIQ+ and other discriminated groups around the world in relation to their possibilities of accessing security and protection and taking advantage of internet and technologies for advancing and exercising their Human Rights and digital freedoms. The strategy should provide room for DDP partners and the overall ecosystem to better support women, LGTBIQ+ and cultural minorities in their inclusion, and self-inclusion, in technology related spaces (online and offline) that support their protection and security.

Enabling inclusion is a question of gender social justice and equality but also of economic and political justice. The increasingly diverse representation in digital security and holistic fields, rapid responders networks, privacy and security tools development, also increases the pool of skilled trainers and developers, among other critical roles. Including women, LGTBIQ+ and other discriminated groups also creates more diversity of profiles using and developing technologies. It enables to oppose the current trend of "digital colonialism" by reflecting a diversity of voices, perspectives and needs. It can also create more opportunities for technologies that are extensive, adaptable and appropriated by many.

Therefore, our strategy for enabling more gender equality and cultural diversity for women, LGBTIQ+ and cultural minorities will encompass learning to analyse our field, programmes and activities through a gender and intersectional lens and also supporting knowledge production and the development of initiatives that are gender and culturally sensitive and appropriated.

2.1 Learning to analyse our field, programs and activities through a gender and intersectional lens

We introduce below key ideas for building a common ground and shared understanding of how gender interplays with our levels of access, uses and practices with technologies. The aim is to understand the specific implications of our activities from a gender and intersectional approach by:

- Acknowledging that gender gaps, discrimination and gender-based violence are both structural and discursive in the way they are deeply embedded in language, narratives, definitions, social structures and laws. These deeply influence the conditions of women, LGTBIQ+ and other discriminated groups in relation to their access to and experience with technology and the Internet.

- Taking into account the economic, political and ecological impact of technologies and how they enable mechanisms of oppression, discrimination or liberation.

- Understanding who DDP actors and partners are on a gender and diversity basis, to monitor for unintended bias in terms of identity factors.

- Understanding how women, LGTBIQ+ and other discriminated groups in different conditions find ways of accessing technologies, and a consideration of how they can protect themselves and others in the process.

- Recognising it is important to make women, LGTBIQ+ and other discriminated groups' experiences and contribution in the development and maintenance of technologies visible.

2.2 Supporting knowledge production and development of gender and culturally sensitive and appropriate initiatives

We introduce below key ideas for areas, initiatives and contents that could be further explored and/or prioritised for enabling more gender equality and cultural diversity in DDP's programs and activities:

- Initiatives that assess and highlight those different contributions and self-inclusion processes in relation to technology access, use and development.

- Initiatives, trainings and programmes that enable women, LGTBIQ+ and other discriminated communities to engage with protection and holistic security.

- Initiatives, trainings and programmes that enable women, LGTBIQ+ and other discriminated communities to engage in the holistic ecosystem of responders to digital emergencies and that contributes to the support and accompaniment of HRDs and Civil Society Organisations.

- Initiatives, trainings and programmes that enable women, LGTBIQ+ and other discriminated communities to engage with free software, internet freedom and infrastructure communities.

- Initiatives, trainings and programmes that are led by women, LGTBIQ+ and cultural minorities themselves and in which these groups are in control of their own protection strategies.

- Initiatives, trainings and learning resources that are culturally and gender-sensitive and contribute to breaking stereotypes and prejudices, through the circulation of new imaginaries and references in relation to gender and tech, the provision of counter-arguments to hate speech, the nurturing of networks of support and solidarity against gender-based violence.

- Initiatives, trainings and programmes that are accessible and open licensed so that more women, LGTBIQ+ and discriminated groups can strengthen their access to trainings and contents that support their Human Rights and digital freedoms (speech, expression, opinion).

- Projects that are oriented towards mid and long term development, as these have more possibilities to generate a positive impact in the sustainability of projects led by women, LGTBIQ+ and other discriminated groups.

- Mechanisms of support for projects and initiatives led by LGTBIQ+, women and discriminated groups that are not registered as legal entities due to increased difficulty in accessing resources or heightened insecurity.

3. Implementation

In order to achieve these different aims and priorities for mainstreaming Gender Equality and Diversity Inclusion into DDP related activities, we will move forward with the creation of the following focus groups and related tasks:

- **Set up a DDP focus group on Strengthening Gender Equality and Diversity Inclusion** during the second quarter of 2019 comprising DDP partners and staff who have experience working on racism, gender and sexual orientation issues. The mandate of this group is to review and update this strategy, recommend us more Sexual Orientation Gender Identities (SOGI) experts included in the DDP vetting and referrals systems and also discuss and inform the implementation of the Gender Equality and Diversity Inclusion strategy recommendations. This will be achieved through regular calls the frequency of which to be defined.

- **Enabling DDP staff to attend a SOGI/GEDI training** in order to implement this strategy in a consistent way with Hivos GEDI policy throughout the DDP programme.

- **Assessing the implications of DDP interventions from a gender and diversity perspective.** DDP will incorporate an assessment of the implications of our interventions for different people, paying special attention to women, LGTBIQ+ and other discriminated groups, in order to address

these differences and other power structures that might create inequality for individuals and communities with regard to their access to security and protection. It is highly recommended to develop formal measures for gender and diversity inclusion built into DDP monitoring and evaluation strategy for the different type of activities supported by DDP (trainings, events, DIF, grants, RRN, etc). Besides, these assessments should be consistent with our Do Not Harm and outreach & impact analysis.

- **Sharing and pushing forward good practices for Gender Equality and Diversity to our partners when planning or coordinating DDP supported activities.** This will be achieved by creating links and partnerships with feminist led holistic security networks and technological infrastructure providers initiatives. As it will be achieved by making our Gender Equality and Diversity Inclusion explicit on our call for proposal, jobs, or any submission to DDP (funding, training or fellowship opportunities). Finally, we will provide to DDP supported events and activities, a set of recommendations regarding gender and cultural sensitive criteria (for selecting participants or creating rapid response networks, use of gender identity descriptions and preferred gender pronouns in events and forms, adoption of explicit code of conducts and anti-harassment policies).